THE MILLENNIUM BUG
Problems and Solutions

The so-called 'Y2K problem' is much bigger than most governments, businesses and the public realise.

by Peter Montague © 1998

First published by
Rachel's Environment & Health Weekly
#604, 25 June; #605, 2 July 1998
Environmental Research Foundation
PO Box 5036
Annapolis, MD 21403-7036, USA

We've been hearing about this problem for some time now, but, like most people, we have been ignoring it. As with many problems, we clip articles about it, then file them for later reference. It's the Y2K problem. To a scientist, "Y" means "year" and "K" means "1,000", so "Y2K" refers to the year 2000 problem. It's a computer problem with possibly serious environment and health implications.

Like most people, we are very suspicious of alarming predictions about the year 2000. What finally focused our attention on the Y2K problem was a small item in the back pages of the *New York Times* of Saturday, June 13, 1998.[1] It began: "The nation's utilities told a Senate panel today [June 12] that they were working to solve expected computer problems when 1999 ends but that they could not guarantee that the lights would not go out on Jan. 1, 2000."

The utilities say the lights may go out. This seems like a problem worth examining.

The *Times* went on: "An informal survey by a Senate panel of 10 of the nation's largest utilities serving 50 million people found none had a complete plan in case its computers failed because of the problem." The *Times* explained: "Many electrical plants use date-sensitive software to run built-in clocks that monitor and control the flow of power. These could fail if not updated."

The utilities say the lights may go out, yet none of them has a full contingency plan. How serious could this problem become?

As we examined the items in our Y2K file, we found opinions ranging all over the place. Some people said, "This is a fake problem invented by people who want to sell fixes." Others said, "This is going to be the end of civilisation as we know it." Where does the truth lie?

I worked five years in the Computing Center at Princeton University, so have more than a passing familiarity with computers. My crystal ball is as hazy as anyone else's, but here is an attempt to offer a realistic look at the nature of this Y2K problem.

Unlike most problems, we know when this one is going to hit us: on January 1, 2000, just a little over 500 days from now.

Here is the crux. Many computers only recognise dates by two digits, e.g., 67 is 1967 and 98 is 1998. But in these computers a 00 date will mean 1900, not 2000, unless their software is rewritten. When such computers start calculating or comparing dates after 1999, they won't work right: they may simply shut down, or they may seem to run fine but produce incorrect information that is very hard to detect.

Computers that have this Y2K problem are called "non-compliant" computers, and it turns out there are quite a few of them.

Many non-compliant computers are the really big "mainframe" machines that serve as the central nervous systems of financial institutions (banks, savings & loans, credit unions), stock exchanges, air traffic control systems, missile defence systems, government tax agencies, the Social Security Administration, the Medicare program, the insurance industry, and all of the *Fortune*-1000 multinational corporations. (And of course, this problem is not limited to the US. Every industrialised country depends heavily upon large mainframe computers.)

A report published by Merrill Lynch, the financial management company, states flatly: "When the millennium arrives, many computer systems and global networks will fail because of an inability to properly interpret dates beyond 1999."[2]

Mainframes will not be the only computers to fail on January 1, 2000 if they are still

non-compliant by then. Many industrial machines contain "embedded systems"—computer chips that are literally embedded within some larger piece of equipment such as in power stations, oil refineries, telephone switches, burglar alarms, emergency room equipment, air traffic control systems, military defence gear and chemical plants, among others.

EMBEDDED COMPUTER CHIPS

By the year 2000 there will be an estimated 25 billion embedded systems, according to the Gartner Group which advertises itself as the world's foremost authority on information technology.[3] By Gartner Group's estimate, two-tenths of one per cent of these 25 billion embedded systems will be non-compliant.[4] Two-tenths of one per cent of 25 billion is 50 million. Therefore the problem, according to the Gartner Group, is to identify and replace those 50 million non-compliant embedded systems in the next 500 days. To solve this problem, someone would have to identify, replace and test about 100,000 chips each day between now and December 31, 1999. Does the US have enough technicians to identify, replace and test 100,000 chips each day? It seems unlikely.

These embedded systems tend to be in the nation's core infrastructure: in the water, sewage and electrical utilities, in railroads and other transportation systems, in hospitals, in police and fire services, in the defence infrastructure, and in petrochemical and other manufacturing plants. But non-compliant computer chips are also embedded in equipment such as photocopiers, telephones, elevators, traffic lights, electric generating plants and nuclear missiles, and they all need to be fixed or replaced.

...non-compliant computer chips are also embedded in equipment such as photocopiers, telephones, elevators, traffic lights, electric generating plants and nuclear missiles...

Byte magazine, a technical computer journal, calls Y2K "a crisis without precedent in human history". It recently reported: "One commonly cited problem is associated with gadgets that monitor periodic maintenance. When the clock strikes 12 midnight on New Year's Eve, 2000, these devices might think it's been 99 years since their last maintenance, realize that's too long for safe operation, and shut down."[5]

Fortune magazine calls it "the biggest screw-up of the computer age"[6] and says it may cost US$1 trillion to fix. (The Vietnam War cost half that much—US$500 billion.)

The Electric Power Research Institute (EPRI)—a trade association for electric utility companies—says the Y2K problem will begin to disrupt businesses, including electric utilities, a year before the new century begins. "Major disruptions in technical and business operations could begin as early as January 1, 1999. Nearly every industry will be affected," EPRI says.[7]

Virginia Hick, who writes a column called "Technology and You" for the St Louis *Post-Dispatch*, recently interviewed Peter de Jager, a well-known Y2K consultant to industry. Here is what Hick wrote:

"...de Jager talked recently with an executive of a company that makes a volatile gas—he would not identify the company more specifically—who told de Jager how his plant discovered the seriousness of faulty embedded chips.

"The plant found a chip that failed when the date was moved forward. When the chip failed, it shut off a valve that would have shut down the cooling system. A cooling system shutdown, the executive said, would have caused an explosion.

"That was great news," de Jager said. "Because they checked, there will be no explosion. They're replacing the chips."

"De Jager worries about the companies that are not checking," Hick wrote.[8]

Conclusion No. 1: If we lived in a community with one or more chemical plants, we would be asking our local government to hold public hearings on the Y2K problem, seeking public assurances from local plant managers that they really have this problem under control. What written plans do they have for assessing these problems, and how large a budget have they committed to solving them? What progress can they demonstrate? Does the plant manager have sufficient confidence in the plant's safety systems to be at the plant with his or her family at midnight, December 31, 1999, to celebrate the new year?

PROGRESS REPORT

Now let's return to the mainframe problem. Because non-compliant computers could harm a company's financial picture (up to and including bankruptcy), on January 12, 1998 the US federal Securities and Exchange Commission (SEC) issued "SEC Staff Legal Bulletin No. 5" which requires publicly held companies to report their progress towards solving their Y2K problems.

On June 10, 1998 Steve Hock, president of Triaxsys Research in Missoula, Montana, testified before the Senate Banking, Housing and Urban Affairs Committee that his company had examined the SEC filings of America's 250 largest corporations.

Mr Hock told the Senate that 114 of the 250 companies had filed no Y2K information with the SEC. Of the 136 companies that *have* filed Y2K information, 101 reported their progress on the assessment phase of the problem. Of these 101, 60 per cent revealed that they have not yet completed their assessments of the Y2K problem.

Mr Hock testified that 36 companies reported their estimated Y2K project costs and how much they had so far spent. The average company reported having spent 21 per cent of the expected total costs of Y2K fixes. Mr Hock concluded: "[The] data show remarkably little progress by the largest US companies in addressing the year 2000 problem. Most of the work has been compressed into an extremely tight window of time. Given the information technology industry's long history of failure to complete large-scale system conversion projects on time, this is cause for serious concern."[9]

The New York Federal Reserve Bank has said that it will take more than a year for a large corporation to test its computers for Y2K compliance *after* all their software has been fixed.[10] This means that all fixes must be completed by September or October of 1998 so testing can begin in time. But many large corporations are still at the stage of assessing the problem, and it's now late June [at the time of writing].

How big is the task for a complex corporation? State Farm Insurance—a company that believes it is on top of the Y2K problem—began working on the problem in 1989 and found that it had 70 million lines of computer code to convert, 475,000 data processing items, more than 2,000 third-party software programs, 900 shared electronic files, plus miscellaneous telephone and

business equipment in 1,550 corporate and regional service facilities. State Farm still has 100 employees working "around the clock" on nothing but Y2K.[11]

But even a forward-looking company like State Farm could be harmed by this problem if its customers, suppliers, partners, bankers and regulators aren't compliant by the year 2000. As Merrill Lynch says: "Even institutions that have fixed their own internal problem will feel the ripple effects from problems occurring externally."[12]

A survey of small businesses by the National Federation of Independent Businesses (NFIB) reported on June 1 that 75 per cent of small businesses have done nothing about the Y2K problem. The NFIB estimates that 330,000 small businesses will go bankrupt and another 370,000 will be "temporarily crippled" by the Y2K problem.[13]

Conclusion No. 2: Portions of the nation's basic infrastructure (utilities, transportation, defence, manufacturing) seem likely to be disrupted by the Y2K problem. Furthermore, parts of the world's core commercial institutions, such as banking and insurance, also seem likely to be disrupted.

ANTICIPATED EFFECTS

If the disruptions don't begin on January 1, 1999, they may begin on July 1, 1999 when fiscal year 2000 begins for 46 out of the 50 states, or on October 1, 1999 when fiscal year 2000 begins for the federal government. But most of the problems will probably surface after midnight on December 31, 1999.

Charles Rossetti, commissioner of the US Internal Revenue Service (IRS), told the *Wall Street Journal* in late April that Y2K is a "very, very serious problem". "There's no point in sugar-coating the problem," he said. "If we don't fix the century-date problem, we will have a situation scarier than the average disaster movie you might see on a Sunday night. Twenty-one months from now, there could be 90 million taxpayers who won't get their refunds, and 95 per cent of the revenue stream of the United States could be jeopardized."[14] Mr Rossetti went on to say he is confident that these problems will not occur because IRS computer experts will prevent them. Critics of IRS are not so sure.[15]

"If we don't fix the century-date problem, we will have a situation scarier than the average disaster movie you might see on a Sunday night."

— Charles Rossetti, commissioner of the US Internal Revenue Service (IRS)

The deadline for having everything fixed—December 31, 1999—is just over 500 days away, and it is an unusual kind of deadline because it cannot be ignored or extended.

Fortune magazine (April 27) reported that, on average, large corporations are only 34 per cent of the way through the job of making their systems compliant.[16]

Government agencies are doing only slightly better. The Government Accounting Office (GAO) stated in March 1998: "Time is running out for solving the Year 2000 problem. Many federal agencies will not be able to renovate and fully test all of their mission-critical systems and may face major disruptions in their operations. At the same time, systems that have been renovated and tested may encounter unanticipated Year 2000 problems."[17]

The GAO gave examples of what may go wrong:

• The nation's air transportation may face major delays and disruptions because the airlines may not be able to file flight plans with the Federal Aviation Administration.

• Taxpayers may not receive timely tax refunds because the IRS may be unable to process their tax returns.

• Payments to veterans and retirees may be delayed or disrupted by the failure of mission-critical systems supporting the nation's benefit payments systems (i.e., people may not receive their social security or disability checks in a timely fashion).

GAO reported on June 10 that 24 government agencies are only 40 per cent of the way towards their goal of Y2K compliance.[18] GAO said it had published 40 reports on government computers during the past two years: "The common theme has been that serious vulnerabilities remain in addressing the federal government's Year 2000 readiness, and that much more action is needed to ensure that federal agencies satisfactorily mitigate Year 2000 risks to avoid debilitating consequences." GAO concluded: "As a result of federal agencies' slow progress, the public faces the risk that critical services could be severely disrupted by the Year 2000 computing crisis."

No one knows what will happen as we approach the year 2000. We do know that many manufacturing processes are dependent upon computers, especially in the chemical processing industries. The *Fortune* report said: "The precision and interdependence of process controls in chemical plants, for instance, make a Rube Goldberg fantasy contraption look simple. Let a single temperature sensor in the complex chain of measuring instruments go cuckoo because of a year 2000 problem, and you'll get a product with different ingredients than you need—if it comes out at all."[19]

Even the nation's defence apparatus could be adversely affected. The GAO reported on June 30 that the US Navy is far behind in fixing its Y2K problems, and concluded: "Failure to address the year 2000 problem in time could severely degrade or disrupt the Navy's day-to-day and, more importantly, mission-critical operations." GAO said the navy doesn't even know how many of its computers have Y2K problems, so it doesn't know how big the task ahead may be.[20]

Why is this seemingly simple problem so difficult? Merrill Lynch, the financial management firm, says there are four reasons:[21]

1. Pervasiveness. Computers that depend on dates are present in every kind of technology—manufacturing systems, medical equipment, elevators, telephone switches, satellites and even automobiles.

2. Interdependence. Computers exchange information among themselves. "A single uncorrected system can easily spread corrupted data throughout an organization and even affect external institutions," Merrill Lynch says.

3. Inconsistency. Computer languages do not store and use dates in a consistent way. Dates are labelled, stored and used in different ways from program to program and even within a single program. Therefore, identifying and correcting dates requires close inspection of the computer code line by line.

4. Size. Most large corporations and government agencies use thousands of programs containing millions of lines of computer code. Each line of code must be inspected manually and, if necessary, fixed.

AND THAT'S NOT ALL...

There are additional reasons why this is a particularly difficult problem. Many business computer programs that run on the largest ("mainframe") computers are written in an obsolete language called "COBOL". COBOL hasn't been taught for 10 years, so there is a distinct shortage of COBOL programmers.[22, 23]

Indeed, there is a shortage of all programmers to work on Y2K problems. Swiss Re (a firm that insures insurance companies against major losses) says: "A total of well over three million programmers would be needed to solve the millennium [date] problem in the US. In actual fact there are only around two million of them at present."[24]

When computer code is rewritten, new errors are introduced at an average rate of one new error in every 14 lines of rewritten code. Thus even "Y2K-compliant" code may not work properly when the time comes.[25]

...it is reasonable to conclude that portions of the nation's critical infrastructure (water, electricity, telecommunications and transportation) may be disrupted for a period...

Therefore, we believe it is reasonable to conclude that portions of the nation's critical infrastructure (water, electricity, telecommunications and transportation) may be disrupted for a period; perhaps a few days, but conceivably longer. Essential government services may also be disrupted.

We could be entirely wrong. However, we believe it is sensible to hope for the best but prepare for the worst.

Individuals might take precautions to protect themselves and their families. They need water, food, shelter and a cash reserve.[26] They need paper records of bank accounts and insurance policies in case computerised records are lost.

But even more importantly, communities need to begin now to think about ways to mitigate these problems. All is not lost. Much trouble can be averted by focused efforts now.

Awareness is the first issue. A recent survey of 643 individuals found that 38 per cent had never heard of the Y2K problem. Among the 400 (62 per cent) who *had* heard of it, 80 per cent said they believed it would be fixed before the year 2000 arrived. This contrasts with an earlier poll of technology and business executives charged with fixing Y2K problems: only 17 per cent of them said they thought the problems would be fixed before the year 2000.[27] People need to be told.

Coordinated action is the second issue. People need the resources to be able to fix their own computers.[28]

Thirdly, communities need to think creatively about ways to help those who are most vulnerable: people who rely on social security, veterans benefits and private pensions, for example. What will happen if their funds are delayed? Local governments, churches and civic groups could begin now to bring communities together to find ways to avert serious problems that might occur. Approached properly, Y2K could become a catalyst for positive community growth and development in the best sense of those words.[29] ∞

About the Author

Peter Montague is Editor of *Rachel's Environment & Health Weekly* and a member of the National Writers Union.

Endnotes

1. "Utilities Say Outages Are Possible in 2000", National News Briefs, *New York Time*s, June 13, 1998, p. 16.
2. See <www.ml.com/woml/forum/millen.htm>.
3. See <http://gartner12.gartnerweb.com/public/static/home/home.html>.
4. Thanks to Roleigh Martin for the Gartner Group estimate. See <http://ourworld.compuserve.com/homepages/roleigh_martin/y2journ.htm>. The most comprehensive, and most pessimistic, web page on Y2K is that of historian Gary North; see <www.garynorth.com>.
5. DeJesus, Edmund X., "Year 2000 Survival Guide", *Byte*, July 1998, pp. 52-62. Good websites covering this problem include: <http://www.yourdon.com>; <www.euy2k.com>; <http://www.year2000.com>; <www.y2ktimebomb.com>; <www.garynorth.com>.
6. Bylinsky, Gene, "Industry Wakes Up to the Year 2000 Menace", *Fortune*, April 27, 1998, pp. 163-180. Available on the web at <www.pathfinder.com/fortune/1998/980427/imt.html>.
7. See <http://year2000.epriweb.com/year2000/challenge.html>.
8. Hick, Virginia, "Expert Warns Computer World is Running Out of Time to Meet 2000; Code is Broken and Needs to Be Fixed Fast, He Says", St Louis *Post-Dispatch*, November 19, 1997, p. C8. See also <www.year2000.com>.
9. Mr Hock's testimony is available at <http://www.senategov/~banking/98_06hrg/061098/witness/hock.htm>.
10. See <www.ny.frb.org/docs/bankinfo/circular/10937.html>.
11. See <www.statefarm.com/about/year.htm>.
12. See <www.ml.com/woml/forum/millen.htm>.
13. See <http://www.amcity.com/sacramento/stories/ 060198/smallb2.html>.
14. Tom Herman, "A Special Summary and Forecast of Federal and State Tax Developments", *Wall Street Journal*, April 22, 1998, p. A1.
15. Pejman, Peyman, "Industry rep voices doubt over federal 2000 readiness", *Government Computer News*, June 15, 1998. See website <www.gcn.com/gcn/1998/June15/industry_rep_voices_doubt_over_f.htm>.
16. Bylinsky, *Fortune*, ibid.
17. Willemssen, Joel C. and Keith Rhodes, "Year 2000 Computing Crisis: Business Continuity and Contingency Planning", GAO/AIMD-10.1.19, General Accounting Office, Washington, DC, March, 1998. Available at <www.gao.gov/y2kr.htm>.
18. Willemssen, Joel C., "Year 2000 Computing Crisis: Actions Must Be Taken Now to Address Slow Pace of Federal Progress", GAO/T-AIMD-98-205, General Accounting Office, Washington, DC, June 10, 1998. Available at <www.gao.gov/y2kr.htm>.
19. Bylinsky, *Fortune*, ibid.
20. Stephenson, John B. et al., "Defense Computers: Year 2000 Computer Problems Put Navy Operations At Risk", GAO/AIMD-98-150, General Accounting Office, Washington, DC, June 1998. Available at <www.gao.gov/y2kr.htm>.
21. See <www.ml.com/woml/forum/millen.htm>.
22. Bylinsky, *Fortune*, ibid.
23. Chandrasekaran, Rajiv, "Older Programmers May Fix Future", *Washington Post*, March 2, 1997, p. A1. See <www.washingtonpost.com/wp-srv/frompost/features/mar97/2000.htm>.
24. See <www.swissre.com/download/public/millene.pdf>.
25. Bylinsky, *Fortune*, ibid.
26. See <www.y2kwomen.com>. If you need this "how to protect your family" information sent to you by mail, send US$2.00 to ERF to cover postage and copying (in the US); we'll mail you 27 pages of information. Please mark your envelope "Y2K".
27. Susan Watson [(508) 935 4190] and Karen Fogerty [(508) 935 4091], "CIO Magazine Study Shows Many Consumers Clueless About Year 2000 Computer Glitch", press release dated June 12, 1998. See <www.cio.com/marketing/releases/y2k_release.html>.
28. DeJesus, *Byte*, ibid.
29. See, for example, Robert Theobald's work on community responses to Y2K: <www.transform.org/transform/tlc/Resiliency.htm>.

Note:

Environmental Research Foundation provides this electronic version of *Rachel's Environment & Health Weekly* free of charge, even though it costs considerable time and money to produce it. Please send your tax-deductible contribution to: Environmental Research Foundation, PO Box 5036, Annapolis, MD 21403-7036, USA. For further information, phone ERF toll free on 1888-2RACHEL (USA only), or (410) 263 1584, or fax on (410) 263 8944.

The Center for Strategic and International Studies (CSIS), a Washington, DC, think-tank, held a conference on 2 June 1998 titled "The Y2K Crisis: A Global Ticking Time Bomb". To complete our Y2K coverage for now, the following is an edited transcript of a conference address given by Mr Alan Simpson on the subject of "Global Food Chains". He is introduced by the conference co-chairman, Mr Arnaud de Borchgrave, director of the CSIS Global Organized Crime Project.

— Editor

Arnaud de Borchgrave: Alan Simpson has conducted briefings and presentations in over 60 countries, and since 1995 this England-born computer and communications advanced technologist has been a leading spokesman on international year 2000 issues.

After 10 years of service with Royal Air Force Intelligence in the UK, where he specialised in electronic warfare, Mr Simpson formed Proloc Computers and Cambridge Advanced Technology. He was a pioneer in advanced communications networks. As president of Satellite Communications Limited, he was one of the early birds in global satellite communications in television, and was awarded nine US Government contracts for satellite links to US embassies.

Mr Simpson also helped develop USIA's much-acclaimed WorldNet during the Reagan administration. He has been a consultant to CNN, BBC, VOA and 13 start-up networks. Since 1995, Mr Simpson added the development of TV news programs to his activities, producing and hosting *Wildfire* and *Countdown 2000*.

Today he will tell us about the Y2K connectivity problem, or what he calls "the global food chain".

Alan Simpson: Thank you, Arnaud.

The year 2000 problem is a global problem. One of the things we've heard said here today, which is spoken a lot in the media, is that the United States is ahead of the rest of the world. Correct. But also it's more dependent on technology than the rest of the world. So while we are ahead in awareness, the effects will be more pronounced here than anywhere else in any country.

Some Third World countries won't even notice it. Other Third World countries, because they use hand-me-down computers from the West, will come to a grinding halt.

The food chain...I'm not speaking about food. The real title should be "the global supply communications and logistics web". But that puts people to sleep, so we call it "the food chain" and then you think you're getting a cooking program.

As an aside from that, since we've been doing this now for about three months, a lot of farmers have contacted me saying, "Are you talking about the real food chain?" And in the first days I said, "No, no, no. We're talking about the relationship between government, major corporations, small corporations and the communications infrastructure." "Oh," said they. "Well, we've got a problem."

A few weeks ago we started looking at this, and it was Bruce Webster [from Object Systems Group] who mentioned in one of his presentations the could-be famine in the United States in 2000. And, like most of you here, I thought, "Rubbish, rubbish!"—until we started looking at the infrastructure and started the wildfire scenarios on "What if?". And looking at New York and California, I walk into a supermarket and I get lettuce, fresh vegetables, any day of the year. Seven days ago they were in a field in California. Now they're in a supermarket just outside New York.

We know the switches on the railroads are faulty. We know because of mergers that even today many of the major corporations in the railroad business don't know where the railway stop is.

When you move this way through, come 2000 you could have a scenario—and when you look at this, it's the Soviet Union in the 1980s—where there's plentiful supply of food in the fields, but you can't get it from the fields to the towns to feed the population. This is not a way-out, whacko scenario. This is for real.

Back to the food chain. When you have a look at it, it's a three-dimensional model. You've got the governments, the major banks, the major corporations, medium and small businesses and mom-and-pop operations. Year 2000 is going to affect this vertical food chain differently at different levels.

Governments have got the resources, but they're sitting around. We are telling each other we're going to be compliant. Yeah, we trust the Pentagon. Yeah, yeah. They're going to be compliant. When we look at the major corporations and the banks, they have the resources and the manpower to correct the problem. Way at the bottom, mom and pop. They can go to manual. Most small businesses can switch their computers off and use pen and pad and go to manual.

But in the middle they have the most problems. And currently, the medium and larger small businesses are being totally neglected with information on year 2000. We focused on the banks. We focused on Wall Street. We focused on General Motors. We have forgotten about the 23 million small and medium businesses that make up the food chain that supplies General Motors.

We don't scream and shout this out because we don't want the world to know this.

So, what have they been sold? Over the '80s they have been sold "just in time". You don't hold stocks. You've all seen the Federal Express ad: all the workers just stand around, and up comes the Fed Ex truck just in time. Most of industry today is waiting for UPS, Fed Ex or someone to come in early, first thing in the morning, to give them work, and they work that day. They don't have stocks. We don't have a stock of strategic commercial materials to keep the country running for one or two months. Everything is just in time: straight out of the ground—they advance shipping and air, communications—straight into the factories. We know that is not going to work. We know! This is not a doomsayer!

We can even tell you the model numbers on the switchers that won't work in the telecommunications network. We can tell you

where they are, and at the moment we know exactly the percentage of the telecom network that will fail. We don't scream and shout this out because we don't want the world to know this. Looking around the world, other countries are in an even worse mess.

But as far as communication is concerned, and I know there are communications people in the room, the year 2000 problem will be the *third* problem between now and 2000.

First, there will be the peak of the micrometeorite shower as predicted by NASA. This event could seriously affect space assets such as telecommunications satellites. There is the possibility that there could be no effect. Every piece of dust or debris could miss the hundreds of orbiting satellites, or impact with little effect. The worst case scenario is that a number of satellites, with their data and voice circuits, could be destroyed or crippled. We need to ensure that the vulnerability lessons learned from *Galaxy IV*—which took out most of the pagers across the United States—have not been forgotten.

The next NASA-predicted event is "Solar Max 23", where the Sun reminds us that it controls our life on Earth. This burst of energy could have tragic, or little effect on the satellites spared by the micrometeorite onslaught. This event, like earlier solar maximum events, could cause disruption in power grids.

Oh, we can use backup power. Problem: the fuel for the backup power is in the ground in tanks. We cannot pump fuel out of underground tanks. If you don't believe me on this, go around to your local filling station. Ask them to take off the panel and show you where the old crank is. In the old pumps, when the power failed you pulled up the front panel, stuck in a starter handle and you could pump for the ambulances and the fire—whatever you wanted. They've taken those out.

Anyone with a name that ends in "president" or "officer" is going to be sued; not *may* be sued, *is* going to be sued.

Going back to the rail system, they've taken out manual points. I talked to some of the major rail companies a few days back and said, "Go to manual." And they said, "All our manual points are in the warehouse up in New York State waiting to be disposed of. We cannot switch manually any more. We have taken out manual reversion systems on most of our key communication, power and switching systems."

So, let's have a look at the communications. Without power and without communications, you can be totally compliant. You can have computer software. It doesn't matter. What can we do about this? We need to start looking seriously and get some true answers.

I met with John Koskinen of the White House yesterday, and we were running through the problems that he had. And the problems that he had are the same as Senator Bennett said [in his presentation]: no one is telling 100 per cent of the truth. Everyone is frightened about their stock position. Everyone is frightened about their credit rating.

I look at the FAA [Federal Aviation Administration]. They're going to get their mainframes delivered—30 of them—in November. They're going to install the software, and they're going to have the system up and running by December. Wow. Let's sell tickets and watch them! [Laughter]

It takes 18 months to put a mainframe on line. And these people are going to do it in 18 days. And I'm going to fly in 2000? Yeah, right. [Laughter]

Come 2000, on the subject of flying, most of the airlines are going to have a 14-day period where the insurance companies will not let them fly. These are real figures.

The legal problem with the year 2000 is probably about US$2 or $3 trillion in litigation. So far, there are 189 lawsuits being settled out of court. Everyone is liable. Anyone with a name that ends in "president" or "officer" is going to be sued; not *may* be sued, *is* going to be sued. The lawyers today are forming task forces. They are set up like military task forces and they are going for class actions. They are going to retire on this.

The year 2000 problem, as far as executive concern goes, is straight negligence. You have known about this for 30 years, and you've done nothing about it. Straight negligence. It's not an act of God. It's man-made.

Not only are communications and power affected. Alarm systems are affected. Security systems are affected. If you want a real wake-up call, how about a look at the threat analysis at one minute past midnight on day one of the year 2000. A lot of the alarm systems in the banks and buildings will be neutralised.

Go back to your offices today and just sit and look around where you have a date/time group; anything on your desk with a date/time group; communications.

Every time you scan your card or put up a palm print, have a look at the printout that comes out on the log. You'll see a date/time group. You request access, cipher, you access it and go. Denied. Go back to the beginning with that date/time group and put two zeroes in there and see what happens. The chances are it will read as an error signal and won't let you in.

Come the year 2000, the security systems in a lot of buildings will not let you in. Passwords are normally for three months and then they're wiped out of the system if they're not used for three months, a month or whatever—depends on how high the security system is. If you crank it forward to 2000 and press the button, you find out no one can get back into it. It won't let you in.

We have created very sophisticated electronic locks on a lot of our communications and access things. They are going to come back and bite us. We have created 2000. We have created a lot of problems.

The communications stuff I don't want to go into too deeply. I would love to do a presentation on communications. But, unfortunately, it'll go out in the world. I don't want every 14-year-old hacker looking and saying, "Well, let's hit a bank. Hey, dude, let's go." That is going to happen. That is the threat side of 2000.

Back to the food chain. So we have a very fragile food chain that goes down. We have communications, we have infrastructure going across.

So the last thing then is this: failure is not an option. Everyone in this room, from government to leadership, has to meet the deadline. Failure for year 2000 is not an option. ∞

Editor's Note:
For the complete transcript of the CSIS conference presentation, visit website <www.csis.org/html/y2ktran.html>, or write to Center for Strategic and International Studies, 1800 K Street, NW, Washington, DC 20006, USA. Also see Alan Simpson's website, <www.comLinks.com>.